DATA PROTECTION POLICY

PROPRIETARY NOTICE

The information contained in this document is proprietary to the **MUA group of companies** (hereinafter referred to as the **"Group"**). The Group consists of:

1. MUA Ltd
2. The Mauritius Union Assurance Cy. Ltd
3. MUA Life Ltd
4. MUA Pension Ltd
5. MUA Mutual Fund Ltd
6. MUA Stockbroking Ltd

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

The primary function of this Data Protection Policy (the "Policy") is to provide a control environment within the Group in terms of the Data Protection Act 2017 ("DPA" or the "Act"). In addition, this Policy has been developed for the promotion of good practice within the Group in relation to the collection, use, processing, handling and storage, amongst others, of personal client data by the employees. Staff members are expected under the Act to understand their role and accountabilities in relation to the enforcement and promotion of good data protection principles in their day-to-day activities.

It is the policy of the Group that all personnel must comply with the policies and process standards as set out in this Policy, unless specific exceptions to the Policy set out herein have been explicitly agreed. Employees are expected to be familiar with these procedures and policies herein included and the specific requirements of applicable laws and rules to their particular areas. Employees should also be aware of, and are expected to conspicuously follow the established internal control procedures which are documented in this Policy.

Employees should review the policies and procedures set forth in this Policy at regular intervals and are required to comply with the spirit and the letter of these written requirements. In order to foster the right data protection culture within the Group, employees may, on ad-hoc basis, be required to provide written confirmation that all policies and internal controls have been complied with.

This Policy is strictly confidential to the MUA Group of Companies and no copies may be made of it either fully or any part thereof. Likewise, no copies of this policy document may be removed from the premises of the Group without the prior written permission of a director of a Company within the Group or of the Head of Group Risk, Legal and Customer Care.

1.2 SANCTIONING LEVELS

Amendments to this Policy are subject to different levels of sanctioning authority listed as follows:

- Minor typographical, numerical or consequential changes, not affecting policy or process will be sanctioned by the Head of Group Risk, Legal and Customer Care.
- Changes to process not affecting intent of the policy will be sanctioned by the Chief Executive Officer in conjunction with the Head of Group Risk, Legal and Customer Care.

The authoritative version of this Policy shall be the electronic version kept with the Legal & Compliance Department of the Group.

1.3 CAUTION

This Policy is not a fully comprehensive document addressing all legal, operational and practical aspects, principles or issues pertaining to or related to the Act. Certain issues and/or aspects of the Act have not been dealt in fully as they still require further definition and/or clarification. These and other issues that will arise afterwards will be addressed and developed in this Policy as and when required over time.

As such, it is expected that the employees are aware that in case of doubt in relation to the Data Protection principles, they should escalate their queries to the Compliance Department; namely to either the Head of Compliance, Mrs. Delphine Ahnee (Ext 517), and/or the two Compliance Specialists, Mrs. Arziana Koyroo (Ext 312) and Mr. Didier Betsy (Ext 184) or by mail on "Grp Compliance" (compliance@mauritiusunion.com).

2 LEGAL IMPLICATIONS

Personal data, which are information relating to an identified or identifiable individual, are collected and used almost every day and everywhere. Personal data can be an individual's name, address, email or mobile number or location data, amongst others.

As the value of personal data grows, the risks to personal data inevitably increase. In addition, with rapid technological change and innovation, controlling personal data is becoming more and more difficult especially with data intensive online activities. The new Act has been enacted to sustain and strengthen the control and personal autonomy of data subjects over their personal data. It has been designed to align with the key principles found in international laws namely the EU General Data Protection Regulation (GDPR) (EU) 2016/679.

A robust Data Protection Policy is of the utmost importance for the good conduct of our business and it is compulsory that you read it carefully. As such, this Policy has been issued to assist employees to implement the spirit and letter of the DPA within their daily operations. It highlights the key challenges and actions that staff members of the Group should consider and adopt to the extent it is practically feasible in order to achieve compliance with the law.

This Policy therefore ensures that the Group:

- complies with the DPA and follows good practice;
- protects the rights of staff, customers, business partners and third parties;
- stores and processes personal data in line with local and foreign laws; and,
- protects itself from the risks of a data or security breaches, amongst others.

3 RISKS FROM NON-COMPLIANCE

It is of critical importance that the policies and standards specified in this document be strictly adhered to by all staff members of the Group. Failure to comply with same may lead to the Group being unnecessarily exposed to a series of non-exhaustive risks linked to data protection breaches.

Any failure to do as outlined, or failure to adhere to its requirements and to the Group-established control policies, procedures and standards will be regarded and treated as a disciplinary matter, including the provision of summary dismissal. Details of all breaches of the rules and disciplinary actions taken will be recorded by the Human Resource Department and/or the Legal & Compliance Department, as the case may be, who will maintain a register for this purpose.

To these ends, all staff members of the Group shall be required to execute an Employee Data Protection Agreement setting out their obligations and general guidelines under the Act.

4 TERMINOLOGY

The following are some key definitions:

"Collect" does not include receive unsolicited information;

"Consent" means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed;

"Controller" means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

"Data subject" means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

"Physical or mental health", in relation to personal data, includes information on the provision of health care services to the individual, which reveals his health status;

"Personal data" means any information relating to a data subject;

"Processing" means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;#

"Processor" means a person who, or public body which, processes personal data on behalf of a controller.

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

"Special categories of personal data", in relation to a data subject, means personal data pertaining to –

(a) his racial or ethnic origin;

(b) his political opinion or adherence;

(c) his religious or philosophical beliefs;

(d) his membership of a trade union;

(e) his physical or mental health or condition;

(f) his sexual orientation, practices or preferences;

(g) his genetic data or biometric data uniquely identifying him;

(h) the commission or alleged commission of an offence by him;

(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or

(j) such other personal data as the Commissioner may determine to be sensitive personal data;

"Third party" means a person or public body other than a data subject, a controller, a processor or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data.

5 PRINCIPLES RELATED TO PROCESSING OF PERSONAL DATA

The object of the DPA is to provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, and manipulate, record or store data relating to individuals.

To this end, the DPA is underpinned by 6 imperative principles (section 21 of the Data Protection Act 2017). Specifically, section 21 of the Act requires that personal data be:

1) processed lawfully, fairly and in a transparent manner in relation to any data subject;
2) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and,
6) processed in accordance with the rights of data subjects.

These principles apply regardless of whether data is stored electronically, on paper or on other materials.

6 POLICY SCOPE

This Policy document applies to all forms of data that the Group may hold in relation to identifiable individuals, even if that information technically may likely fall outside the scope of the DPA. These forms include and are not restricted to the following categories of personal data in relation to a data subject:

(a) names;
(b) residential addresses;
(c) email addresses;
(d) telephone numbers;
(e) racial or ethnic origin;
(f) political opinion or adherence;
(g) religious or philosophical beliefs;
(h) membership of a trade union;

(i) his physical or mental health or condition;

(j) his sexual orientation, practices or preferences;

(k) his genetic data or biometric data uniquely identifying him;

(l) the commission or alleged commission of an offence by him;

(m) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or

(n) such other personal data as the Commissioner may determine to be sensitive personal data;

(o) any other information of a personal nature permitting the identification of an individual.

7 LAWFULNESS, FAIRNESS AND TRANSPARENCY

As a matter of policy, the Group regards the lawful and correct treatment of personal information as indispensable in maintaining the confidence of those with whom we deal with. Staff members shall ensure at all times that personal data are collected only for the requirements of our business and only if the collection of the data is necessary for that purpose.

7.1 DATA LIMITATION

Every staff member of the Group has the responsibility for ensuring that data are collected, stored and handled appropriately and as per the set procedures stated herein.

Personal data must at all times be collected for explicit, specified and legitimate purposes and not further processed in a way incompatible with those purposes. As such, each staff member, business unit and/or department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles mentioned therein.

7.2 DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Staff members will, through stringent self-management and application of criteria and controls:

1) Observe strict rigour regarding the fair collection and use of information;

2) Specify the purposes for which information is being collected and used by a Company of the Group;

3) Collect and process appropriate information, and only to the extent that it is needed to fulfil their business and operational needs or to comply with any legal requirements;
4) Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
   i. The right to be informed that processing is being undertaken;
   ii. The right of access to one's personal information;
   iii. The right to prevent processing in certain circumstances; and,
   iv. The rights to correct, rectify, block or erase information which is regarded as wrong information.
5) Take appropriate technical and organisational security measures to safeguard clients' personal information; and,
6) Ensure that personal information is not transferred abroad without suitable safeguards.

However, staff members have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that the Group meets its legal obligations.
- The Legal & Compliance Department shall, as and when required, be responsible for:
  1) Keeping the board updated about data protection responsibilities, risks and issues;
  2) Reviewing all data protection procedures and related policies, in line with an agreed schedule;
  3) Arranging data protection training and advice for the people covered by this Policy;
  4) Handling data protection questions from staff and anyone else covered by this Policy;
  5) Dealing with requests from individuals to see the data the Group holds about them (also called "subject access requests"); and,
  6) Checking and approving any contracts or agreements with third parties that may handle the Group's sensitive data.

7.3 GENERAL STAFF GUIDELINES

1) The only people able to access data covered by this Policy should be those who need it for their work.
2) Personal data must not be shared informally. When access to confidential information is required, employees shall request it from their line managers.
3) Employees should keep all data secure, by taking sensible precautions and following the standards of this Policy.

4) In particular, strong passwords must be used and they should never be shared.
5) Personal data should not be disclosed to unauthorised people, either within the Group or externally.
6) Data should be regularly reviewed and updated if they are found to be out of date. If no longer required, they should be deleted and disposed of.
7) Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
8) When working with personal data, employees should ensure the screens of their personal computers and laptops are always locked when left unattended.
9) Employees, laptops users in particulars, should not save copies of personal data to personal pen drives and other removable media without proper encryption.

8 CONSENT

Consent is any freely given, specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which s/he signifies his/her agreement to personal data relating to him/her being processed.

8.1 WHY IS CONSENT IMPORTANT?

Consent is one of the lawful bases for the processing of personal data. Given our willingness to continuously remain a DPA-compliant financial institution, the Group will make every effort to give its clients ongoing control over how we use their data, thus ensuring that our organisation is thoroughly transparent and accountable.

Handling consent therefore builds customer trust and engagement and enhances the reputation of our operations. Relying on inappropriate or invalid consent could destroy trust, harm our reputation and might leave our Group exposed to substantial fines.

Thus, when dealing with clients, staff members shall constantly have in mind the key elements of consent: it must be ***freely given***, ***specific, informed*** and there ***must be an indication signifying agreement***.

At the time of collection, data subjects should be readily informed about the right to withdraw their consent at any time. Consent shall therefore be:

1) **specific, and unambiguous**; by setting out the purpose of the various phases of the processing;
2) **informed**; data subjects should be informed about the right to withdraw their consent at any time;

3) **clear**; easy to withdraw without affecting the lawfulness of processing; as well as,

4) **verifiable**; appropriate records shall be kept to demonstrate what the individual has consented to, including what they were told, when and how they consented.

8.1.1 Collection of consent

Consent shall be collected at the outset of establishing a client relationship whereby the prospective client shall be requested to fill-in the Consent Form appended at Appendix 6 of this Policy.

8.1.2 When consent is not required?

Somehow, there are certain specific cases provided for in section 28 of the Act where consent is not required. Staff shall process clients' personal data only if:

(a) the data subject consents to the processing for one or more specified purposes;

(b) the processing is necessary –

1) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
2) for compliance with any legal obligation to which the controller is subject;
3) in order to protect the vital interests of the data subject or another person;
4) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
5) the performance of any task carried out by a public authority;
6) the exercise, by any person in the public interest, of any other functions of a public nature;
7) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
8) for the purpose of historical, statistical or scientific research.

8.2 PERSONAL DATA OF CHILDREN

In terms of section 30 of the Act, staff members shall not process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian. As such, staff members should obtain consent from whoever holds parental responsibility for them.

As a rule, Know Your Customer and Customer Due Diligence ("KYC/CDD") measures shall be conducted on the child's parent or guardian to verify that the person giving the own consent in these circumstances is lawfully authorised to do so and doing so in the interests and benefits of the child.

9 RIGHTS OF DATA SUBJECTS

Section 37 of the Act provides that "*every controller shall, on the written request of a data subject provide, at reasonable intervals, without excessive delay and, subject to subsection (7), free of charge, confirmation as to whether or not personal data relating to the data subject are being processed and forward to him a copy of the data.*"

The above rights include the rights to access, rectify, erase and restrict the processing of personal data. The principle of "fair and transparent" processing means a client must be provided all relevant information in relation to the processing of his/her data, unless s/he already has this information**.**

Where the staff member obtains personal data directly from the data subject, the latter should be informed of the following rights under the law:

1) The purpose/s for which the data are being collected;
2) The intended recipients of the data;
3) Whether or not the supply of the data by that data subject is voluntary or mandatory;
4) The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
5) The existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;

6) The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
7) The period for which the personal data shall be stored;
8) The right to lodge a complaint with the Data Protection Commissioner;
9) Where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and
10) Any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data are collected.

However, where the controller does not obtain personal data directly from the client, the latter shall, as soon as reasonably practicable, be informed of his/her rights.

10 RIGHT OF INFORMATION AND ACCESS

An individual has the right to:

1) obtain confirmation whether his/her personal data are being processed;
2) access the data (i.e. to a copy); and
3) be provided with supplemental information about the processing.

Access rights are intended to allow individuals to check the lawfulness of processing and the right to have a copy of their personal data. However, these rights should not adversely affect the rights of others.

10.1.1 How should such request/s be handled?

A written request must be made to the Data Protection Officer of the Group by the data subject. A copy of the requested information will be provided without excessive delay and free of charge. Such confirmation shall include whether or not personal data relating to the data subject are being processed.

Depending on the request of the client, or in case the request is manifestly excessive, the Group may charge a reasonable fee for providing the required information or taking the actions requested by the client.

10.2 RIGHT OF RECTIFICATION

An individual has the right to:

1) rectify inaccuracies in personal data held about him/her.
2) complete incomplete data; and,
3) record a supplementary statement.

10.3 RIGHTS OF ERASURE

In line with section 41 of the Act, the Group has the right to erase personal data in the following circumstances:

1) The data are no longer necessary in relation to the purpose for which they were collected or otherwise processed.
2) The data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing.
3) The data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing.
4) The personal data have been unlawfully processed.

In such instances, the Group will also forthwith inform its authorised third parties processing the personal data that the data subjects have requested the erasure of any links to, or copy or replication of, their personal data.

However, such requests shall not be complied with where the processing of personal data is necessary for:

1) reasons of public interest in the field of public health
2) the purpose of historical, statistical or scientific research
3) compliance with a legal obligation to process the personal data to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or,
4) the establishment, exercise or defence of a legal claim.

10.4 RIGHT TO OBJECT

Data subjects have the right to object in writing at any time to the processing of personal data concerning them. For example, clients have the right to object to direct marketing which includes profiling.

For the avoidance of doubt, profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict certain aspects concerning that person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

10.5 EXERCISE OF RIGHTS

A data subject can, at any time, exercise his/her rights to access, rectify, erase or object to the processing of his/her personal data. The Group will therefore also use reasonable means to verify the identity of the person making the request but should not keep or collect data just so as to be able to meet subject access requests. Data subjects will be required to fill-in and returned a signed copy of the Rights of Data Subject Form, as annexed to Appendix 5.

11 PERSONAL DATA BREACHES

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, client's personal data being either transmitted, stored or otherwise processed.

In terms of Section 25 and 26 of the Act, the Group shall, without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a client, the Group shall, after prior communication the Data Protection Commissioner, communicate the personal data breach to the client.

12 TRANSFER OF PERSONAL DATA OUTSIDE MAURITIUS

Personal data can be transferred to another country provided that the Group has put in place appropriate safeguards with respect to the protection of the personal data and complies with both the conditions of transfer established in section 36 of the DPA and the requirements of the Information Exchange Policy set out in the Group's Information Security Policy.

13 DATA STORAGE

Personal data will be stored securely and will only be accessible to authorised staff. Information will be stored in compliance with the provisions of the Act and the Group's Data Retention Policy and Data Disposal Policy.

When data is stored on paper, it should be classified and kept securely where unauthorised people cannot access or see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reasons:

1) When not required, the paper or files should be kept in a locked drawer or filing cabinet.
2) Employees must make sure that paper and printouts are not left in places where unauthorised people could see them, like on a printer.
3) Data printouts should be disposed of as per the Data Disposal Policy.

When data is stored electronically, it must be protected as per the guidelines set out in the Group's Information Security Policy. These include but are not limited to the following:

1) Data should be protected by strong passwords that are changed regularly and never shared between employees.
2) If data is stored on removable media (like a CD, DVD or portable storage drives or devices), these should be kept locked away securely when not being used.
3) Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
4) Servers containing personal data should be sited in a secure location, away from general office space.
5) Data should be backed up frequently. Those backups should be tested regularly, in line with the Group's standard backup procedures.
6) Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
7) All servers and computers containing data should be protected by approved security software and a firewall.

Questions about safe data storage shall be directed to the IT Department, the Legal & Compliance Department and/or the Data Protection Officer, as the case may be.

14 DATA PSEUDONYMISATION

Data pseudonymisation, as defined in the Act, means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

By correctly pseudonymising or anonymising its data, the Group will have the ability to share, disseminate or publish a greater amount of personal data with fewer restrictions. Personal identifiers such as name, address, date of birth, reference number, amongst others, are removed from the data source thus allowing the information to be used for secondary purposes and made available within a controlled environment to other government agencies and/or local authorities for historical scientific research or for statistical purposes.

14.1 Anonymisation

Anonymisation is the process of removing, obscuring, aggregating and/or altering any identifiers in a dataset which can point to the particular person(s) the data relate(s) to. In addition to the legal requirement to share information with government or local authorities, the Group has additional regulatory obligations to ensure transparency in its processes and, as such, routinely publishes and distributes information as appropriate. As and when required, the Group will therefore anonymise personal data in the course of its normal business activities.

14.2 Anonymisation process

The anonymisation process will be strictly restricted to the IT department of the Group. Therefore, the concerned staff will:

1) proceed with the anonymisation in such a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate security (technical) or organisational measures; and,
2) strictly abide to appropriate safeguards with respect to the protection and storage of the anonymised data.

15 DATA ACCURACY AND CLEAN DESK POLICY

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In addition, it is the responsibility of each employee to take reasonable steps to ensure that personal data are:

1) held in as few places as necessary. Staff should not create any unnecessary additional data copies or sets.
2) updated at every available opportunity. For instance, by confirming a customer's details when s/he calls.
3) updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

16 PHOTOGRAPHS, ID CARDS AND CAMERAS

16.1 Use of photographs

This policy has been written in such a way to ensure that MUA complies with the legal requirements pertaining to the use of staff images. Therefore, in order to discharge its legal and regulatory obligations and responsibilities as an employer, MUA may from time to time collect, keep and display the photographs of its staff for management, administrative and identification purposes. Similarly, staffs are aware that these photographs may be displayed within the Group's network and/or premises such as via email, intranet or on Staff Cards for evidential purposes. The use of photographs for in compliance with the Company's policies and or approved processes are to part of the scope of work of the staff and ought to be complied to by all staff.

Staffs' names, images and/or photographs may from time to time be used and displayed in the press (newspapers, magazines and so on.), on television, on social networking sites/forums or via other medias/networks for advertising, promotional and such other related purposes.

All employees of MUA hereby acknowledge that their images and photographs shall be collected, stored, used and processed strictly in line with the Act and it is a condition of their employment to strictly abide to such MUA standards, rules, regulations and policies currently in force or which may from time to time be issued by MUA.

16.2 Use of staff and visitor's cards

For security and evidential purposes, all employees and visitors to MUA premises must be readily identifiable. This means that logistics, security and reception should be able to identify any individual accessing any MUA premises, usually by comparing their face to the photograph on their Staff Card. For this reason, while on any premises of MUA, staff and visitors must wear their staff or visitors' cards and these must be clearly visible.

MUA's logistics and security staff shall have the right to ask individuals to identify themselves by comparison with their photograph on their ID card.

16.3 What information is held?

Information collated from a staff's Card activity, when it is used to gain access to MUA, shall be collected, processed and stored by the Group's security access control systems. The information that is recorded comprises the date and time at which a reader has scanned the Staff Card. Information collected are the person's name, photo, department, access levels and such information as may be necessary and proportionate for identification and security purposes. The data is held on a server managed by IT Department.

For visitors, the only information that will be recorded at the reception desk is the name of the visitor, purpose of visit, time-in and time-out, person or persons being met and such other relevant and proportionate information as may be required or necessary for identification and security purposes only.

16.4 Why is this information held?

The primary purpose of implementing staff cards is to monitor their attendance and provide a secured access to staffs to MUA offices and to different departments/clusters.

The information will also be recorded for the purpose of investigating incidents where knowing who was in an area at a particular time would be of assistance.

16.5 How long will this information be held for?

The processing of Staff Card data regarding access will be held for as long as is necessary for identification, traceability and security purposes only. This shall allow the Information Systems and Logistics department a reasonable amount of time to carry out any investigation in circumstances when an incident has occurred.

16.6 Who can access this information?

The data is only accessible by authorised members of the Human Resource and Information Systems and Logistics departments. Furthermore, access to the back-up tapes for the purposes of an investigation can only be authorised by the Group's Head of Information Systems & Logistics and the Group Head of Legal and Compliance or in their absence, the Manager of the Logistics Department and the Data Protection Officer. It is understood that one of these two Senior Managers shall always be part of the decision. If this is not possible the case will be referred to the Group HR.

16.7 Use of cameras

MUA operates a video surveillance system within and around its premises through the Information Security and Logistics department. The function of this camera monitoring system is to assist in the detection and deterrence of crime and to assist the Police and other relevant authorities in the event of a major emergency. In compliance with the Act, the system will be operated in such a

way so as to safeguard the rights of data subjects as stipulated under Section 9 of this Policy.

All video surveillance images have ownership and copyright vested in MUA. Recorded images and videos will normally be preserved for a 30 days-period or for as long as is necessary for identification, traceability, security and evidential purposes by MUA.

Camera images and videos are only accessible to the Logistics Manager and will only be accessed in the case of an investigation needing to be carried out.

16.8 Review of procedures

The recording and retention of data collected from Staff and/or Visitor's Identity Cards activity will be regularly monitored in order to ensure that it is achieving its purpose. If procedures are found not to be achieving their purpose then they will be modified.

17 RESPONSIBILITY OF THE INFORMATION SYSTEMS AND LOGISTICS DEPARTMENT

The Information Systems and Logistics Department shall, amongst other things, be responsible for:

1) ensuring that all systems, services and equipment used for storing data comply with the data security standards set out in the Act;
2) performing regular checks and scans to ensure security hardware and software are functioning properly;
3) evaluating any third-party services the Group is considering using to store or process data. For instance, third party/external service providers; and
4) performing and carrying out any tasks and implementing any procedures necessary for the protection of personal data within all systems of the Group.

18 CONTACT US

18.1 Name and contact details of the Group's Data Protection Officer:

Mrs. Arziana KOYROO

Legal and Compliance Department

Telephone: 207 5500 (Ext: 312)

18.2 Complaints and queries

If you have any queries or complaints about our compliance with this Policy, or if you would like to make any complaints to us, you may contact the Data Protection Officer either by emailing us on **DPO@mua.mu.**

Or by writing to us at:

Data Protection Officer

4, Léoville l'Homme Street,

Port Louis

Mauritius

To help us handle your request quickly, you may alternatively submit your recommendations, comments or complaints by completing this online form at **mua.mu.**

19 UPDATES AND AMENDMENTS

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Act.

20 APPENDIX 1 – WITHDRAWAL OF CONSENT

20.1 Procedure for Withdrawal of Consent

- Step 1: Client fills in and duly signs the withdrawal form which is available from the company's website on **mua.mu**.
- Step 2: Withdrawal form is submitted to the Data Protection Officer (DPO).
- Step 3: The DPO communicates the withdrawal of consent request to the Group's IT & Marketing Department.
- Step 3: Formal letter as notification is sent to client to acknowledge his/her request of withdrawal of consent and that his/her documents shall/have been destroyed accordingly.

Please refer to sections 7 and 8 of this Policy for further guidance.

20.2 Withdrawal form

The full withdrawal form is available for download at **mua.mu**.

21 APPENDIX 2 - PROCEDURES IN CASE OF PERSONAL DATA BREACHES

21.1 Procedure for Personal Data Breach & Communication to Data subjects

- Step 1: Personal data breach occurs.
- Step 2: DPO informs the Data Protection Commissioner within 72hrs of the breach.
- Step 3: DPO simultaneously notify the Data Subject of the breach unless same falls under the exempted circumstances.
- Step 4: Corrective actions are undertaken.

Please refer to sections 7 and 8 of this Policy for further guidance.

21.2 Personal Data Breach Notification Form

The full Personal Data Breach form is available for download from **mua.mu**.

22 APPENDIX 3 - PROCEDURES TO DESTROY PERSONAL DATA

Where the purpose for keeping the personal data has lapsed, the Group will as soon as is reasonably practicable, destroy the data. In addition, data subjects shall be required to fill in and submit a signed Rights of Data Subject Form as annexed to Appendix 5 of this Policy.

23 APPENDIX 4 - PROCEDURE IN CASE OF OBJECTION FROM DATA SUBJECT

- Step 1: Objection received in writing from data subject.
- Step 2: Direct the objection to the DPO.
- Step 3: DPO analyses whether there is any compelling legitimate grounds for the processing which override the Data Subject's interests, rights and freedom.
- Step 4: If no, procedures for withdrawal of consent and destruction of personal data are followed.
- Step 5: If yes, notify client that we have legitimate grounds for the processing of his/her data.

In addition, data subjects can objet to the processing of their personal data by filling-in and submitting a signed Rights of Data Subject Form as annexed to Appendix 5 of this Policy.

24 APPENDIX 5 – RIGHT OF DATA SUBJECTS FORM

The full Rights of Data Subjects Form is available for download from **mua.mu**.

25 APPENDIX 6 – DATA PROTECTION CONSENT FORM

The full Data Protection Consent Form is available for download from **mua.mu**.